A SYNOPSIS

OF THE PROPOSED THESISI ENTITLED

‘CONSTRUCTION AND PROPERTIES OF THE LINEAR CODES BASED ON SOME SPECIAL FUNCTIONS’

SUBMITTED TO THE

SWAMI RAMANAND TEERTH MARATHWADA UNIVERSITY, NANDED.

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

UNDER THE FACULTY OF SCIENCE

BY

Shaikh Wajid Majid

M.Sc. (Mathematics)

UNDER THE GUIDANCE

OF

Dr. Rupali S. Jain

Associate Professor

School of Mathematical Sciences,

SRTM, University, Nanded-431606

1. Abstract:

In this research work, we study about the linear codes and construction of linear codes by several functions. We also discuss about parameters of the constructed code and optimality of the code.

2. Introduction/ Choice of the topic with reasoning: -

'Algebraic coding theory is a branch of Engineering with roots in mathematics and application to Computer science. Linear code is a topic in coding theory.

Definition 2.1: Any non-empty finite set of symbols is called alphabet. A word over alphabet is simply a finite set of sequence of elements in alphabets. Let A^* be the set of all words over alphabet then any subset C of A^* is called code over given alphabet. To be even more simple, a q-ary code is a code whose alphabets has cardinality q.

Example: Let $A = Z_2 = \{0, 1\}$, $A^* = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ then $C = \{(0, 0), (0, 1)\}$ is called a code whose alphabet is Z_2 and A^* is called set of words.

Definition 2.2: The Hamming distance between v,w in C (code) is $d(v, w) = |\{i \mid v_i \neq w_i, 1 \leq i \leq n\}|$. The Hamming weight of v in C is defined as number of non-zero coordinate in the vector v and denoted by wt(v). The distance *d* of a linear code is the minimum weight of its nonzero codeword's, or equivalently, the minimum distance between distinct codeword's.

Example: $Z_2 = \{0, 1\}$, $C = \{(0, 0), (0, 1), (1, 1)\}$ here $wt((0, 1)) = 1$, $wt((1, 1)) = 2$ and $d((0, 0), (1, 0)) = 1$, $d((0,1), (1, 1)) = 1$. And $d(C) = 1$.

Definition 2.3: Let q be a power of prime. A linear [n,k,d;q] code over F_q is k- dimension subspace of F_q^n with distance d. A linear code Cover F_q is called cyclic if $(c_0, c_1, \ldots, c_{n-1})$ is in C implies that $(c_{n-1}, c_0, \ldots, c_{n-2})$ is in C.

Example: $Z_2 = \{0, 1\}$ and consider Z_2^3 as vector space then $C = \{(0, 0, 0), (0, 0 1)\}$ is a linear code with parameters [3, 1, 1].

Definition 2.4: Let $D = \{d_1, d_2, \ldots, d_n\}$ is a subset of GF(q). Let tr denote the trace function from GF(q) to GF(p) through we define, $C_D = \{tr(xd_1), tr(xd_2), \ldots, tr(xd_n) \mid x \text{ in } GF(q)\}$ is a linear code and D is called the defining set of this code C_D.

Definition 2.5: Let A_i denote the number of codeword's with Hamming weight i in a linear code C of length n. The weight enumerate of C is defined by $1 + A_1Z + A_2Z^2 + \quad + A_nZ^n$. And $(A_1, A_2, \ldots, A_n)$ is called the weight distribution of a code C.

Definition 2.5: Any matrix M is called generator matrix of a given linear code C if the row space of that matrix generate the linear code C as a subspace. Any matrix N is called a parity-check matrix of a given code C if N is the generator matrix for its dual.

3. An overview of the relevant literature: -

As the linear code is very useful topic in Mathematics, Computer science, Graph theory, many of the researchers start working on this area. Kelan Ding and Cunsheng Ding work on 'A Class of two-weight and three-weight codes and their applications in secret sharing'. Cunsheng Ding, Chunlei Li, Nian Li, and Zhengchun Zhou give some results on 'Three weight cyclic codes and their weight distribution. Ji Yuan and Cunsheng Ding worked on 'Secrete sharing schemes.

Peter Beelen, Sudhir R. Ghorpade, Sartaj Ul Hasan contributed to 'Linear codes associated to determine verities. The paper by K.Wang determines the dimension and generator polynomial of some cyclotomic codes, which involve special monomials. The paper by K. Abdulkhalikov and S. Mesnager is a nice survey on connections among bent functions that are linear on elements of some classical spreads, semi fields and over polynomials. Bent function have been used to construct codes in number of the literature, the paper by Z. Heng and Q. Yue employee Bent function over the ring Z_4 to construct codeword's meeting the Levenshtein bound. Many of the Institute and research center start working on it just like IIT Bombay, DRDO etc. It has huge application in computer science so some people also start their work on linear codes. Swanand Kadheand Robert Calderbank gives the paper on 'Rate optimal binary linear locally repairable codes with small availability' which gives us application of coding theory in computer science.

5. Objectivities of the Research

Some of our objectives are as follows,

- To construct a linear code with help of special function like Trace function, Bent Quadratic function, and some other special functions
- To discuss characterization, parameters and optimality of constructed codes.
- To find properties of Generator and Parity-check matrix of a constructed code.
- To give bounds for constructed codes
- In some cases, dual of the code have good parameters as compare to code so we explain some of the properties of dual code like self-orthogonal.
- We take some non-planar, perfect non-linear function and some other interesting functions to construct a code because it gives relation between code and some group.
- We check from which kind of function gives as special code like cyclic code, self-dual, etc.

- Most of the work done on finite field with two elements so we try to construct a code with the help of different finite set of symbols like finite field more than two elements, finite rings, etc.
- We also try to give properties of the code as module that gives interrelation between Coding theory and Algebra.
- Weight distribution is hot research topic in Coding theory so we take different class of codes with different weight and discuss its weight distribution. We also think about algebraic structure on class of code and its properties.
- We discuss about the application of Coding in different subjects like Computer science, Graph theory, Number theory, etc.

4. Methodology:

For the above-mentioned study, first of all we have to study basic Coding theory, some results related to decoding rules. We take the help of research papers to understand the parameter codes, minimality condition for codes, optimality condition of codes. We also have to study properties of Finite fields, basic points in Discrete Mathematics, some concepts of Linear Algebra and properties of polynomials. We also take the help of some basic terms in Algebraic geometry, Cryptography, Representation theory of finite group, Commutative algebra and Graph theory.

Weight distribution is crucial in coding theory so we deeply study of it from different books and from recent research papers on weight distribution of codes. We study the nature of the special functions like Trace function, Bent quadratic function etc., to construct new linear codes which have good parameters. We also take the help of Bounds in coding theory for finding bounds to our constructed codes.

6. Significance of the study:

Coding theory widely used in Computer science, Communication system and many more another branches. Some of the applications of our topics are as follows,

- A class of two weight and three weight codes over GF(q) have applications in authentication codes, association codes and strongly regular graphs, in addition to their application in consumer electronic, communication and data storage system.

- Linear codes with only a few weights are interesting in theory for many reasons for example projective two weights codes and strongly regular graphs are equivalent.
- Cyclic codes have been an important of both Mathematics and Engineering for decades. They have been widely used in consumer electronic, data transmission, broadcast system and computer application as they have efficient encoding and decoding algorithm.
- Cyclic codes with a few weights are also special interest in designing hopping sequences.
- Every electronic device we own uses a code which is defined using a Galois field.

6. Plan of Research Work:

Sr. No	Period	Plan of the work	Targets to be achieved
1	First year	Read some books on basic coding theory, Number theory, Linear algebra, etc.	Good command on the subject
2	Second year	Study of course work and some books on advanced coding theory. Also refer some research paper on our topic	To clear the course work and to understand the research papers related our topic.
3	Third Year	Work on some problems to be included in the thesis.	Submit at least two papers.
4	Fourth Year	Publishing some papers and submitting the Thesis.	Submit some more papers and Thesis submission.

8. References:

1) A. E. Ashikhmin. Generalized hamming weights for Z4-linear codes. In Proc. Of the 1994 IEEE Int. Symp. Inform. Theory, page 306, 1994.

2) A. E. Ashikhmin. On generalized hamming weights for Galois ring linear codes. Designs, Codes and Cryptography, 14:107–126, 1998.

3) A. Bonneeaze and I. M. Duursma. Translates of linear codes over Z4. IEEE Trans. Inform. Theory, 43(4):1218–1230, 1997.

4) A.Bonnecaze, P.Sol´e,and A.R.Calderbank Quaternary quadratic residue codes and unimodular lattices. IEEE Trans. Inform. Theory,41:366–377, 1995.

5) S. Boztas, A. R. Hammons, and P. V. Kumar. 4-phase sequences with nearoptitum correlation properties. IEEE Trans. Inform. Theory,38(3):1101–1113,1992.
6) P. Delsarte and J. M. Goethals. Alternating bilinear forms over GF(q). J. Comb.Theory, 19:26–50, 1975.
7) Zhengchun Zhou, Nian Li, Cuiling Fan, Tor Helleseth. Linear codes with two or three weights from quadratic Bent function.
8) Qiuyan Wang, Kelan Ding, Dongdai Lin, Rui Xue. A kind of three weight linear codes.
9) J. L. Massey and T. M. Mittelholzer. Convolutions codes over rings. In Proceedings of the Fourth Joint Swedish-USSR Int. Workshop in Inform. Theory,Sweden, 1989.
10) A. Ashikhmin, A. Barg, G. Cohen, and L. Huguet. Variations on minimal codewords in linear codes. In Proc. of the 11th Int. Symp. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, pages 96–105.Springer-Verlag, 1995.
11) Kelan Ding and Cunsheng Ding. A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing.
12) Cunsheng Dinga, Chunlei Lib, Nian Lic, Zhengchun Zhoud. Three-weight cyclic codes and their weight distributions.
13) Jin Yuan and Cunsheng Ding, Senior Member, IEEE. Secret Sharing Schemes From Three Classes of Linear Codes.
14) Peter Beelena, Sudhir R. Ghorpadeb, Sartaj Ul Hasanc. Linear codes associated to determinantal varieties.
15) G. R. Blakley and C. Meadows. Security of ramp schemes. In Advances in Cryptology - CRYPTO ‘84, volume 196 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1985.
16) C. Blundo, A. D. Santis, and U. Vaccaro. Efficient sharing of many secrets. In STACS 93, volume 665 of Lecture Notes in Computer Science.Springer Berlin Heidelberg, 1993.
17) A. Braeken, V. Nikov, and S. Nikova. On cheating immune secret sharing. In Proc. 25th Symposium on Information Theory in the Benelux, pages 113–120, 2014.
18) P. D’Arco, W. Kishimoto, and D. Stinson. Properties and Constraints of Cheating-Immune Secret Sharing Schemes. Discrete Applied Mathematics,154:219–233, 2006.

19) C. Ding and J. Yuan. Covering and Secret Sharing with Linear Codes. In Discrete Mathematics and Theoretical Computer Science, volume 2731 of Lecture Notes in Computer Science, pages 11–25. Springer-Verlag, 2003.
20) D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. Journal of the ACM, 40(1):17–47, 1993.

Signature	**Signature**
Research Scholar	**Research Guide**
Mr. Shaikh Wajid Majid	**Dr. Rupali S. Jain**

Place: - Nanded

Date: -